

Context-free rewriting systems and word-hyperbolic structures with uniqueness

Alan J. Cain & Victor Maltcev

[AJC] Centro de Matemática, Universidade do Porto,
Rua do Campo Alegre 687, 4169-007 Porto, Portugal

Email: ajcain@fc.up.pt

Web page: www.fc.up.pt/pessoas/ajcain/

[VM] School of Mathematics & Statistics, University of St Andrews,
North Haugh, St Andrews, Fife KY16 9SS, United Kingdom

Email: victor@mcs.st-andrews.ac.uk

ABSTRACT

This paper proves that any monoid presented by a confluent context-free monadic rewriting system is word-hyperbolic. This result then applied to answer a question asked by Duncan & Gilman by exhibiting an example of a word-hyperbolic monoid that does not admit a word-hyperbolic structure with uniqueness (that is, in which the language of representatives maps bijectively onto the monoid).

1 INTRODUCTION

Hyperbolic groups — groups whose Cayley graphs are hyperbolic metric spaces — have grown into one of the most fruitful areas of group theory since the publication of Gromov’s seminal paper [Gro87]. The concept of hyperbolicity generalizes to semigroups and monoids in more than one way. First, one can consider semigroups and monoids whose Cayley graphs are hyperbolic [Cai, CS09]. Second, one can use Gilman’s characterization of hyperbolic groups using context-free languages [Gilo2]. This characterization says that a group G is hyperbolic if and only if there is a regular language L (over some generating set) of normal forms for G such that the language

$$M(L) = \{u\#_1 v\#_2 w^{\text{rev}} : u, v, w \in L \wedge uv =_G w\}$$

(where w^{rev} denotes the reverse of w) is context-free. (The pair $(L, M(L))$ is called a *word-hyperbolic structure*.) Duncan & Gilman [DG04] pointed out that this characterization generalizes naturally to semigroups and monoids. The geometric generalization gives rise to the notion of *hyperbolic* semigroup; the

Acknowledgements: The first author’s research was funded by the European Regional Development Fund through the programme COMPETE and by the Portuguese Government through the FCT (Fundação para a Ciência e a Tecnologia) under the project PEst-C/MAT/Ul0144/2011 and through an FCT Ciência 2008 fellowship.

linguistic one to the notion of *word-hyperbolic* semigroups. While the two notions are equivalent for groups [DGo4, Corollary 4.3] and more generally for completely simple semigroups [FKo4, Theorem 4.1], they are not equivalent for general semigroups. This paper is concerned with *word-hyperbolic* semigroups.

Some of the pleasant properties of hyperbolic groups do not generalize to word-hyperbolic semigroups. For example, hyperbolic groups are always automatic [ECH⁺92, Theorem 3.4.5]; word-hyperbolic semigroups may not even be *asynchronously* automatic [HKOTo2, Example 7.7]. On the other hand, word-hyperbolicity for semigroups is independent of the choice of generating set [DGo4, Theorem 3.4], unlike automaticity for semigroups [CRRTo1, Example 4.5].

Duncan & Gilman [DGo4, Question 2] asked whether every word-hyperbolic monoid admits a word-hyperbolic structure where the language of representatives L projects *bijectively* onto the monoid. By analogy with the case of automatic groups [ECH⁺92, § 2.5] and semigroups [CRRTo1, p. 380], such a word-hyperbolic structure is called a *word-hyperbolic structure with uniqueness*. The question also applies to semigroups; Duncan & Gilman have a particular interest in the situation for monoids because a positive answer in that case would imply that the class of word-hyperbolic semigroups is closed under adjoining an identity.

As explained in [Subsection 2.1](#) below, every hyperbolic group admits a word-hyperbolic structure with uniqueness. Furthermore, every automatic semigroup admits an automatic structure with uniqueness [CRRTo1, Corollary 5.6].

The main goal of this paper is to give a negative answer to the question of Duncan & Gilman by exhibiting an example of a word-hyperbolic monoid that does not admit a word-hyperbolic structure with uniqueness ([Example 4.2](#)). En route, however, a result of independent interest is proven: that any monoid presented by a confluent context-free monadic rewriting system is word-hyperbolic ([Theorem 3.1](#)).

2 PRELIMINARIES

This paper assumes familiarity with regular languages and finite automata and with context-free grammars and languages; see [HU79, Chs 2–4] for background reading and for the notation used here.

The empty word (over any alphabet) is denoted ε .

2.1 Word-hyperbolicity

DEFINITION 2.1. A *word-hyperbolic structure* for a semigroup S is a pair $(L, M(L))$, where L is a regular language over an alphabet A representing a finite generating set for S such that L maps onto S , and where

$$M(L) = \{u\#_1v\#_2w^{\text{rev}} : u, v, w \in L \wedge uv =_S w\}$$

(where $\#_1$ and $\#_2$ are new symbols not in A and w^{rev} denotes the reverse of the word w) is context-free. The pair $(L, M(L))$ is a *word-hyperbolic structure with uniqueness* if L maps bijectively onto S ; that is, if every element of S has a unique representative in L .

A semigroup is *word-hyperbolic* if it admits a word-hyperbolic structure.

A group is hyperbolic in the sense of Gromov [Gro87] if and only if it admits a word-hyperbolic structure ([Gil02, Theorem 1] and [DGo4, Corollary 4.3]). Furthermore, every group admits a word-hyperbolic structure with uniqueness: if $(L, M(L))$ is a word-hyperbolic structure for a group G , then the fellow-traveller property is satisfied [DGo4, Theorem 4.2] and so L forms part of an automatic structure for G [ECH⁺92, Theorem 2.3.5]. Therefore there exists an automatic structure with uniqueness for G , where the language of representatives L' is a subset of L [ECH⁺92, Theorem 2.5.1]. Hence $(L', M(L) \cap L' \#_1 L' \#_2 (L')^{\text{rev}})$ is a word-hyperbolic structure with uniqueness for G .

2.2 Rewriting systems

This subsection contains facts about string rewriting needed later in the paper. For further background information, see [BO93].

A *string rewriting system*, or simply a *rewriting system*, is a pair (A, \mathcal{R}) , where A is a finite alphabet and \mathcal{R} is a set of pairs (ℓ, r) , known as *rewriting rules*, drawn from $A^* \times A^*$. The single reduction relation $\Rightarrow_{\mathcal{R}}$ is defined as follows: $u \Rightarrow_{\mathcal{R}} v$ (where $u, v \in A^*$) if there exists a rewriting rule $(\ell, r) \in \mathcal{R}$ and words $x, y \in A^*$ such that $u = x\ell y$ and $v = xry$. That is, $u \Rightarrow_{\mathcal{R}} v$ if one can obtain v from u by substituting the word r for a subword ℓ of u , where (ℓ, r) is a rewriting rule. The reduction relation $\Rightarrow_{\mathcal{R}}^*$ is the reflexive and transitive closure of $\Rightarrow_{\mathcal{R}}$. The process of replacing a subword ℓ by a word r , where $(\ell, r) \in \mathcal{R}$, is called *reduction*, as is the iteration of this process.

A word $w \in A^*$ is *reducible* if it contains a subword ℓ that forms the left-hand side of a rewriting rule in \mathcal{R} ; it is otherwise called *irreducible*.

The string rewriting system (A, \mathcal{R}) is *noetherian* if there is no infinite sequence $u_1, u_2, \dots \in A^*$ such that $u_i \Rightarrow_{\mathcal{R}} u_{i+1}$ for all $i \in \mathbb{N}$. That is, (A, \mathcal{R}) is noetherian if any process of reduction must eventually terminate with an irreducible word. The rewriting system (A, \mathcal{R}) is *confluent* if, for any words $u, u', u'' \in A^*$ with $u \Rightarrow_{\mathcal{R}}^* u'$ and $u \Rightarrow_{\mathcal{R}}^* u''$, there exists a word $v \in A^*$ such that $u' \Rightarrow_{\mathcal{R}}^* v$ and $u'' \Rightarrow_{\mathcal{R}}^* v$.

The string rewriting system (A, \mathcal{R}) is *length-reducing* if $(\ell, r) \in \mathcal{R}$ implies that $|\ell| > |r|$. Observe that any length-reducing rewriting system is necessarily noetherian. The rewriting system (A, \mathcal{R}) is *monadic* if it is length-reducing and the right-hand side of each rule in \mathcal{R} lies in $A \cup \{\varepsilon\}$; it is *special* if it is length-reducing and each right-hand side is the empty word ε . Observe that every special rewriting system is also monadic.

A special or monadic rewriting system (A, \mathcal{R}) is *context-free* if, for each $a \in A \cup \{\varepsilon\}$, the set of all left-hand sides of rules in \mathcal{R} with right-hand side a is a context-free language.

Let (A, \mathcal{R}) be a confluent noetherian string rewriting system. Then for any word $u \in A^*$, there is a unique irreducible word $v \in A^*$ with $u \Rightarrow_{\mathcal{R}}^* v$ [BO93, Theorem 1.1.12]. The irreducible words are said to be in *normal form*. The monoid presented by $\langle A \mid \mathcal{R} \rangle$ may be identified with the set of normal form words under the operation of ‘concatenation plus reduction to normal form’.

The subscript symbols in the derivation and one-step derivation relations $\Rightarrow_{\mathcal{R}}^*$ and $\Rightarrow_{\mathcal{R}}$ for a rewriting system \mathcal{R} are never omitted in this paper, in order to avoid any possible confusion with the derivation and one-step derivation relations \Rightarrow_{Γ}^* and \Rightarrow_{Γ} for a context-free grammar Γ .

3 MONOIDS PRESENTED BY CONFLUENT CONTEXT-FREE MONADIC REWRITING SYSTEMS

THEOREM 3.1. *Let (A, \mathcal{R}) be a confluent context-free monadic rewriting system. Then $(A^*, M(A^*))$ is a word-hyperbolic structure for the monoid presented by $\langle A \mid \mathcal{R} \rangle$.*

Proof. Let M be the monoid presented by $\langle A \mid \mathcal{R} \rangle$. Let

$$K = \{u\#_2v^{\text{rev}} : u, v \in A^*, u =_M v\}.$$

Let $\phi : (A \cup \{\#_1, \#_2\})^* \rightarrow (A \cup \{\#_1\})^*$ be the homomorphism extending

$$\#_1 \mapsto \varepsilon, \quad \#_2 \mapsto \#_2, \quad a \mapsto a \text{ for all } a \in A.$$

Then $M(A^*) = K\phi^{-1} \cap A^*\#_1A^*\#_2A^*$. Since the class of context-free languages is closed under taking inverse homomorphisms, to prove that $M(A^*)$ is context-free it suffices to prove that K is context-free.

For each $a \in A \cup \{\varepsilon\}$, let $\$a$ and $\tilde{\$}a$ be new symbols. Let

$$\begin{aligned} \$_{A \cup \{\varepsilon\}} &= \{\$a : a \in A \cup \{\varepsilon\}\} & \$A &= \{\$a : a \in A\}, \\ \tilde{\$}_{A \cup \{\varepsilon\}} &= \{\tilde{\$}a : a \in A \cup \{\varepsilon\}\} & \tilde{\$}A &= \{\tilde{\$}a : a \in A\}, \end{aligned}$$

and for any word $w = w_1 \cdots w_n$ with $w_i \in A$, let $\$w$ and $\tilde{\$}w$ be abbreviations for $\$w_1 \cdots \w_n and $\tilde{\$}w_1 \cdots \tilde{\$}w_n$ respectively.

For each $a \in A \cup \{\varepsilon\}$, let $\Gamma_a = (N_a, A, P_a, O_a)$ be a context-free grammar such that $L(\Gamma_a)$ is the set of left-hand sides of rewriting rules in \mathcal{R} whose right-hand side is a . Since \mathcal{R} is length-reducing, no $L(\Gamma_a)$ contains ε . Therefore assume without loss of generality that no Γ_a contains a production whose right-hand side is ε [HU79, Theorem 4.3].

Modify each Γ_a by replacing each appearance of a terminal letter $b \in A$ in a production by $\$b$; the grammar $\Gamma'_a = (N'_a, \$_{A \cup \{\varepsilon\}}, P'_a, O'_a)$ thus formed has the property that $w \in L(\Gamma_a)$ if and only if $\$w \in L(\Gamma'_a)$. Modify each Γ_a by reversing the right-hand side of every production in P_a and by replacing each appearance of a terminal letter $b \in A$ in a production by $\tilde{\$}b$; the grammar $\Gamma''_a = (N''_a, \$_{A \cup \{\varepsilon\}}, P''_a, O''_a)$ thus produced has the property that $w \in L(\Gamma_a)$ if and only if $\tilde{\$}w^{\text{rev}} \in L(\Gamma''_a)$.

The language

$$\{\$p\#_2\tilde{\$}p^{\text{rev}} : p \in A^*\}$$

is clearly context-free. (Notice that $\$p$ can either be an abbreviation for a non-empty word $\$p_1 \cdots \p_k or the single letter $\$_\varepsilon$, and similarly for $\tilde{\$}p^{\text{rev}}$.) Let $\Delta = (N_\Delta, \$A \cup \tilde{\$}A\{\#_2\}, P_\Delta, O_\Delta)$ be a context-free grammar defining this language. Assume without loss of generality that the various non-terminal alphabets N'_a , N''_a and N_Δ are pairwise disjoint.

Define a new context-free grammar $\Theta = (N_\Theta, A \cup \{\#_2\}, P_\Theta, O_\Theta)$ by letting

$$N_\Theta = N_\Delta \cup \$_{A \cup \{\varepsilon\}} \cup \tilde{\$}_{A \cup \{\varepsilon\}} \cup \bigcup_{a \in A \cup \{\varepsilon\}} (N'_a \cup N''_a),$$

and

$$P_\Theta = P_\Delta \cup \left[\bigcup_{a \in A \cup \{\varepsilon\}} (P'_a \cup P''_a) \right] \cup \{ \$a \rightarrow \$a\$_\varepsilon, \$a \rightarrow \$_\varepsilon\$a, \tilde{\$}a \rightarrow \tilde{\$}a\$_\varepsilon, \tilde{\$}a \rightarrow \$_\varepsilon\tilde{\$}a : a \in A \cup \{\varepsilon\} \} \quad (3.1)$$

$$\cup \{ \$a \rightarrow O'_a, \tilde{\$}a \rightarrow O''_a : a \in A \cup \{\varepsilon\} \} \quad (3.2)$$

$$\cup \{ \$a \rightarrow a, \tilde{\$}a \rightarrow a : a \in A \cup \{\varepsilon\} \}. \quad (3.3)$$

Notice that elements of $\$_{A \cup \{\varepsilon\}}$ now play the rôle of non-terminals, while in the various grammars Γ'_a and Γ''_a , they were terminals. Notice further that the start symbol of Θ is O_Δ .

The aim is now to show that $L(\Theta) = K$.

LEMMA 3.2. *If $w \in L(\Theta)$, then $w = u\#_2v^{\text{rev}}$ for some $u, v \in A^*$, and there exists some $p \in A^*$ such that $\$_p \Rightarrow_\Theta^* u$ and $\tilde{\$}_{p^{\text{rev}}} \Rightarrow_\Theta^* v^{\text{rev}}$.*

Proof. Let $w \in L(\Theta)$. Then $O_\Delta \Rightarrow_\Theta^* w$, and the first production applied is from P_Δ . Since no production in $P_\Theta - P_\Delta$ introduces a non-terminal symbol from N_Δ , assume that all productions from P_Δ in the derivation of w are carried out first, before any productions from $P_\Theta - P_\Delta$. This shows that there is some word $q \in L(\Delta)$ such that $O_\Delta \Rightarrow_\Theta^* q \Rightarrow_\Theta^* w$. By the definition of Δ , it follows that $q = \$_p\#_2\tilde{\$}_{p^{\text{rev}}}$ with

$$O_\Delta \Rightarrow_\Theta^* \$_p\#_2\tilde{\$}_{p^{\text{rev}}} \Rightarrow_\Theta^* w.$$

Since symbols from $\$_{A \cup \{\varepsilon\}} \cup \tilde{\$}_{A \cup \{\varepsilon\}}$ can ultimately only derive symbols from A (and not the symbol $\#_2$), it follows that there exist $u, v \in A^*$ with $\$_p \Rightarrow_\Theta^* u$ and $\tilde{\$}_{p^{\text{rev}}} \Rightarrow_\Theta^* v^{\text{rev}}$ such that $w = u\#_2v^{\text{rev}}$. \square

LEMMA 3.3. *Let $w, u \in A^*$. If $w \Rightarrow_{\mathcal{R}}^* u$, then $\$_u \Rightarrow_\Theta^* \$_w$.*

Proof. Suppose

$$w = w_0 \Rightarrow_{\mathcal{R}} w_1 \Rightarrow_{\mathcal{R}} w_2 \Rightarrow_{\mathcal{R}} \dots \Rightarrow_{\mathcal{R}} w_n = u$$

is a sequence of rewriting of minimal length from w to u .

Proceed by induction on n . If $n = 0$, it follows that $w = u$ and there is nothing to prove. So suppose $n > 0$ and that the result holds for all shorter such minimal-length rewriting sequences. Then $w_0 \Rightarrow_{\mathcal{R}} w_1$, and so $w_0 = x\ell y$ and $w_1 = xay$ for some $x, y \in A^*$, $a \in A \cup \{\varepsilon\}$, and $(\ell, a) \in \mathcal{R}$. So $\ell \in L(\Gamma_a)$. Hence, first applying a production of type (3.2), the construction of Γ'_a and the inclusion of all its productions in Θ shows that

$$\$_a \Rightarrow_\Theta O'_a \Rightarrow_\Theta^* \$_\ell. \quad (3.4)$$

By the induction hypotheses, $\$_u \Rightarrow_\Theta^* \$_{w_1}$. Now consider the cases $a \in A$ and $a = \varepsilon$ separately:

1. $a \in A$. Then $\$_{w_1} = \$_x\$_a\$_y$ and so

$$\begin{aligned} \$_u &\Rightarrow_\Theta^* \$_{w_1} && \text{(by the induction hypothesis)} \\ &= \$_x\$_a\$_y \\ &\Rightarrow_\Theta^* \$_x\$_\ell\$_y && \text{(by (3.4))} \\ &= \$_{w_0} \\ &= \$_w. \end{aligned}$$

2. $a = \varepsilon$. Then $\$_{w_1} = \$_x\$_y$ and so by (3.4),

$$\begin{aligned} \$_u &\Rightarrow_\Theta^* \$_{w_1} && \text{(by the induction hypothesis)} \\ &\Rightarrow_\Theta^* \$_x\$_y \\ &\Rightarrow_\Theta \$_x\$_a\$_y && \text{(by (3.1))} \\ &\Rightarrow_\Theta^* \$_x\$_\ell\$_y && \text{(by (3.4))} \\ &= \$_{w_0} \\ &= \$_w. \end{aligned}$$

This completes the proof. \square

LEMMA 3.4. Let $u, w \in A^*$. If $\$u \Rightarrow_{\Theta}^* \w , then $w \Rightarrow_{\mathcal{R}}^* u$.

Proof. The strategy is to proceed by induction on the number n of productions of type (3.1) or (3.2) in the minimal-length derivation of $\$w$ from $\$u$.

Suppose such a minimal length derivation involves a production $\$_{\varepsilon} \rightarrow \varepsilon$ (of type (3.3)). If this symbol $\$_{\varepsilon}$ is introduced by a production of type (3.1), then the derivation would not be of minimal length. So this symbol $\$_{\varepsilon}$ must be present in $\$u$, which, by the definition of the abbreviation $\$u$ requires $u = \varepsilon$. But this would mean that the derivation produced ε , which contradicts the hypothesis of the lemma. So the derivation does not involve productions $\$_{\varepsilon} \rightarrow \varepsilon$.

The only productions where symbols from $\$_{A \cup \{\varepsilon\}}$ appear on the left-hand side are of types (3.1), (3.2), and (3.3). Since there are no productions $\$_{\varepsilon} \rightarrow \varepsilon$, any production of type (3.3) would produce a terminal symbol, which is impossible. So the first production applied in the derivation sequence must be of type (3.1) or (3.2).

Suppose first that $n = 0$. Then there is no possible first production and thus $\$w = \u , which entails $w = u$ and so there is nothing to prove.

Suppose now that $n > 0$ and that the result holds for all shorter such minimal-length derivations. Consider cases separately depending on the whether the first production applied in the derivation is of type (3.1) or (3.2):

1. Type (3.1). So $\$u = \$x\$y \Rightarrow_{\Theta} \$x\$_{\varepsilon}\y for some $x, y \in A^*$ with $xy = u$. The symbol $\$_{\varepsilon}$ thus produced does not derive ε since no production $\$_{\varepsilon} \rightarrow \varepsilon$ is involved. So $\$x \Rightarrow_{\Theta}^* \w' , $\$_{\varepsilon} \Rightarrow_{\Theta}^* \w'' , $\$y \Rightarrow_{\Theta}^* \w''' , where $w = w'w''w'''$, where $w', w''' \in A^*$ and $w'' \in A^+$ and all three of these derivations involve fewer than n productions of type (3.1) or (3.2). By the induction hypothesis, $w' \Rightarrow_{\mathcal{R}}^* x$, $w'' \Rightarrow_{\mathcal{R}}^* \varepsilon$, and $w''' \Rightarrow_{\mathcal{R}}^* y$, and thus $w = w'w''w''' \Rightarrow_{\mathcal{R}}^* xy = u$.
2. Type (3.2). So $\$u = \$x\$_a\$y \Rightarrow_{\Theta} \$xO'_a\y for some $x, y \in A^*$ with $xay = u$. Now, O'_a is the start symbol of Γ'_a , and $L(\Gamma'_a)$ consists of words of the form $\$_{\ell}$ where $\ell \Rightarrow_{\mathcal{R}} a$. Thus

$$\$u \Rightarrow_{\Theta} \$xO'_a\$y \Rightarrow_{\Theta}^* \$x\$_{\ell}\$y \Rightarrow_{\Theta}^* \$w.$$

Thus $\$x \Rightarrow_{\Theta}^* \w' , $\$_{\ell} \Rightarrow_{\Theta}^* \w'' , and $\$y \Rightarrow_{\Theta}^* \w''' , where $w', w'', w''' \in A^*$ are such that $w = w'w''w'''$, and each of these derivation sequences involve fewer than n productions of type (3.1) or (3.2). Hence by the induction hypothesis, $w' \Rightarrow_{\mathcal{R}}^* x$, $w'' \Rightarrow_{\mathcal{R}}^* \ell$, and $w''' \Rightarrow_{\mathcal{R}}^* y$. Therefore

$$w = w'w''w''' \Rightarrow_{\mathcal{R}}^* x\ell y \Rightarrow_{\mathcal{R}} xay = u.$$

This completes the proof. \square

LEMMA 3.5. For any $u, w \in A^*$ $w \Rightarrow_{\mathcal{R}}^* u$ if and only if $\$u \Rightarrow_{\Theta}^* \w .

Proof. Suppose $w \Rightarrow_{\mathcal{R}}^* u$. Then $\$u \Rightarrow_{\Theta}^* \w by Lemma 3.3. By $|w|$ applications of productions of type (3.3), $\$w \Rightarrow_{\Theta}^* w$. So $\$u \Rightarrow_{\Theta}^* w$.

Suppose that $\$u \Rightarrow_{\Theta}^* w$. Only productions of type (3.3) have terminals on the right-hand side. So $\$u \Rightarrow_{\Theta}^* \$w \Rightarrow_{\Theta}^* w$. So by Lemma 3.4, $w \Rightarrow_{\mathcal{R}}^* u$. \square

Reasoning symmetric to the proofs of [Lemmata 3.3, 3.4, and 3.5](#) establishes the following result:

LEMMA 3.6. *For any $u, w \in A^*$ $w \Rightarrow_{\mathcal{R}}^* u$ if and only if $\tilde{\$}_{u^{\text{rev}}} \Rightarrow_{\Theta}^* w^{\text{rev}}$.*

Suppose $u\#_2v^{\text{rev}} \in K$. Then $u, v \in A^*$ and $u =_M v$. Therefore there is a normal form word p with $u \Rightarrow_{\mathcal{R}}^* p$ and $v \Rightarrow_{\mathcal{R}}^* p$. So by [Lemmata 3.5 and 3.6](#), $\$ _p \Rightarrow_{\Theta}^* u$ and $\tilde{\$}_{p^{\text{rev}}} \Rightarrow_{\Theta}^* v^{\text{rev}}$. Since every production in P_{Δ} is included in P_{Θ} , it follows that

$$O_{\Delta} \Rightarrow_{\Theta}^* \$ _p \#_2 \tilde{\$}_{p^{\text{rev}}},$$

whence $O_{\Delta} \Rightarrow_{\Theta}^* u\#_2v^{\text{rev}}$ and so $u\#_2v^{\text{rev}} \in L(\Theta)$.

Conversely, suppose $w \in L(\Theta)$. By [Lemma 3.2](#), there are words $u, v, p \in A^*$ with $w = u\#_2v^{\text{rev}}$, $\$ _p \Rightarrow_{\Theta}^* u$, and $\tilde{\$}_{p^{\text{rev}}} \Rightarrow_{\Theta}^* v^{\text{rev}}$. By [Lemmata 3.5 and 3.6](#), it follows that $u \Rightarrow_{\mathcal{R}}^* p$ and $v \Rightarrow_{\mathcal{R}}^* p$. So $u =_M v$ and thus $w = u\#_2v^{\text{rev}} \in K$.

Hence $L(\Theta) = K$. Thus K and so $M(A^*)$ are context-free. Therefore $(A^*, M(A^*))$ is a word-hyperbolic structure for the monoid M . \square

4 WORD-HYPERBOLIC STRUCTURES WITH UNIQUENESS

This section exhibits an example of a word-hyperbolic monoid that does not admit a word-hyperbolic structure with uniqueness.

The following preliminary result, showing that admitting a word-hyperbolic structure with uniqueness is not dependent on the choice of generating set, is needed. The proof is similar to that of the independence of word-hyperbolicity from the choice of generating set [[DGo4](#), Theorem 3.4], but the detail and exposition are different to make clear that uniqueness is preserved. Additionally, the result here also shows that whether one deals with monoid or semigroup generating sets is not a concern.

PROPOSITION 4.1. *Let M be a monoid that admits a word-hyperbolic structure with uniqueness over either a semigroup or monoid generating set, and let A be a finite alphabet representing a semigroup or monoid generating set for M . Then there is a language L such that (A, L) is a word-hyperbolic structure with uniqueness for M .*

Proof. Suppose S admits a word-hyperbolic structure (B, K) . For each $b \in B$, let $u_b \in A^*$ be such that $u_b =_M b$. (If A represents a semigroup generating set, ensure that u_b lies in A^+ ; this restriction is important only if b is actually the identity.) Let $\mathcal{P} \subseteq B^* \times A^*$ be the rational relation:

$$\mathcal{P} = (\{(b, u_b) : b \in B\})^*$$

Notice that if $(v, w) \in \mathcal{P}$, then $v =_M w$.

Let

$$L = K \circ \mathcal{P} = \{w \in A^* : (\exists v \in K)((v, w) \in \mathcal{P})\};$$

observe that L is a regular language. Notice that, by the definition of \mathcal{P} , for each word v in K there is exactly one word $w \in L$ with $(v, w) \in \mathcal{P}$. Since for each $x \in M$ there is exactly one word v in K with $v =_M x$, it follows that there is exactly one word $w \in L$ with $w =_M x$. That is, the language L maps bijectively onto M .

Let \mathcal{Q} be the rational relation

$$\mathcal{P}(\#_1, \#_1)\mathcal{P}(\#_2, \#_2)\mathcal{P}^{\text{rev}}.$$

Then $M(L) = M(K) \circ \mathcal{Q}$ and so $M(L)$ is a context-free language.

Thus (A, L) is a word-hyperbolic structure for S in every case except when S is a monoid, A is a semigroup generating set, and the representative in K of the identity is ε . In this case, let $L_1 = (L - \{\varepsilon\}) \cup \{e\}$, where $e \in A^+$ represents the identity. Then L_1 is contained in A^+ and maps bijectively onto S . The language $M(L_1)$ is context-free: a pushdown automaton recognizing it can be constructed from one recognizing $M(L)$ by modifying it to read e instead of the empty word as one of the multiplicands or result while simulating reading the empty word whenever e is encountered. \square

EXAMPLE 4.2. Let $A = \{a, b, c, d\}$ and let $\mathcal{R} = \{(ab^\alpha c^\alpha d, \varepsilon) : \alpha \in \mathbb{N}\}$. Let M be the monoid presented by $\langle A \mid \mathcal{R} \rangle$. Then M is word-hyperbolic but does not admit a regular language of unique representatives and thus, in particular, does not admit a word-hyperbolic structure with uniqueness.

Proof. Let G be the language of left-hand sides of rewriting rules in \mathcal{R} . The language G is context-free, and so (A, \mathcal{R}) is a context-free special rewriting system. Two left-hand sides of rewriting rules in \mathcal{R} only overlap if they are exactly equal, and so (A, \mathcal{R}) is confluent. Hence, by [Theorem 3.1](#), $(A^*, M(A^*))$ is a word-hyperbolic structure for the monoid M . So M is word-hyperbolic. Identify M with the language of normal form words of (A, \mathcal{R}) .

Suppose for *reductio ad absurdum* that M admits a word-hyperbolic structure with uniqueness. Then, by [Proposition 4.1](#), there is a regular language L over A such that $(L, M(L))$ is a word-hyperbolic structure with uniqueness for M . In particular, every element of M has a unique representative in L . Let \mathcal{A} be a finite state automaton recognizing L and let n be the number of states in \mathcal{A} .

Now, if $w \in L$ represents $u \in M$, then $w \Rightarrow_{\mathcal{R}}^* u$: the word u can be obtained from w by replacing subwords lying in G by the empty word, which effectively means deleting subwords that lie in G . Consider this process in reverse: the word w can be obtained from u by inserting words from G .

If a word from G is inserted between two letters of u , call it a *depth-1* inserted word. If a word from G is inserted between two letters of a depth- k inserted word, it is called a depth- $(k+1)$ inserted word. A word inserted immediately before the first letter or immediately after the last letter of a depth- k inserted word also counts as a depth- k inserted word. See the following example, where for clarity symbols from u are denoted by x :

$$x \overbrace{ab \text{ } \overbrace{abbccd}^{\text{depth 2}} \text{ } bccd}^{\text{depth 1}} \overbrace{abbccd}^{\text{depth 1}} xx \overbrace{abbbcccd}^{\text{depth 1}} xx.$$

Then it is possible to obtain w from u by performing all depth-1 insertions first, then all depth-2 insertions, and so on until w is reached.

Suppose that, in order to obtain w from u , a word $ab^\alpha c^\alpha d \in G$ is inserted for some $\alpha > n$. Let $w = w'aw''dw'''$, where these distinguished letters a and d are the first and last letters of this inserted word. Notice that $w'' \Rightarrow_{\mathcal{R}}^* b^\alpha c^\alpha$, since

$$w = w'aw''dw''' \Rightarrow_{\mathcal{R}}^* w'ab^\alpha c^\alpha dw''' \Rightarrow_{\mathcal{R}} w'w''' \Rightarrow_{\mathcal{R}}^* u.$$

(Of course, w'' may or may not contain inserted words of greater depth.) Since α exceeds n , the automaton \mathcal{A} enters the same state immediately after reading two different symbols b of this inserted word, say after read-

ing $w'apb$ and $w'apbqb$. Similarly it enters the same state immediately after reading two different symbols c of this inserted word, say after reading $w'apbqbrc$ and $w'apbqbrcsc$. Therefore by the pumping lemma, w factors as $w'apbqbrcsctdw'''$ such that

$$w'apb(qb)^i rc(sc)^j tdw''' \in L$$

for all $i, j \in \mathbb{N} \cup \{0\}$, where the subwords p and q consist of letters b (members of this inserted word) and possibly also inserted words of greater depth, the subwords s and t consist of letters c (members of this inserted word) and possibly also inserted words of greater depth, and the subword r consists of some letters b followed by some letters c (members of this inserted word) and possibly also inserted words of greater depth. Thus

$$p \Rightarrow_{\mathcal{R}}^* b^{\beta_1}, \quad q \Rightarrow_{\mathcal{R}}^* b^{\beta_2}, \quad r \Rightarrow_{\mathcal{R}}^* b^{\beta_3} c^{\gamma_3}, \quad s \Rightarrow_{\mathcal{R}}^* c^{\gamma_2}, \quad t \Rightarrow_{\mathcal{R}}^* c^{\gamma_1},$$

where $\beta_1 + \beta_2 + \beta_3 + 2 = \gamma_1 + \gamma_2 + \gamma_3 + 2 = \alpha$. It follows that

$$\begin{aligned} & w'apb(qb)^i rc(sc)^j tdw''' \\ \Rightarrow_{\mathcal{R}}^* & w'ab^{\beta_1} b(b^{\beta_2} b)^i b^{\beta_3} c^{\gamma_3} c(c^{\gamma_2} c)^j c^{\gamma_1} dw''' \\ = & w'ab^{\alpha + (\beta_2 + 1)(i-1)} c^{\alpha + (\gamma_2 + 1)(j-1)} dw'''. \end{aligned}$$

Set $i = \gamma_2 + 2$ and $j = \beta_2 + 2$ to see that

$$w'apb(qb)^{\gamma_2+1} rc(sc)^{\beta_2+1} tdw''' \in L$$

and

$$\begin{aligned} & w'apb(qb)^{\gamma_2+1} rc(sc)^{\beta_2+1} tdw''' \\ \Rightarrow_{\mathcal{R}}^* & w'ab^{\alpha + (\beta_2 + 1)(\gamma_2 + 1)} c^{\alpha + (\gamma_2 + 1)(\beta_2 + 1)} dw''' \\ \Rightarrow_{\mathcal{R}}^* & w'w'' \quad (\text{since } ab^{\alpha + (\beta_2 + 1)(\gamma_2 + 1)} c^{\alpha + (\gamma_2 + 1)(\beta_2 + 1)} d \in G) \\ \Rightarrow_{\mathcal{R}}^* & u. \end{aligned}$$

So there are two distinct words w and $w'apb(qb)^{\gamma_2+1} rc(sc)^{\beta_2+1} tdw''$ in L representing the same element u of M . This is a contradiction and so shows the falsity of the supposition that the insertion of a word $ab^\alpha c^\alpha d$ with $\alpha > n$ is used in obtaining the representative in L from a normal form word in M .

Let $G' = \{ab^\alpha c^\alpha d : \alpha \leq n\}$. Then obtaining a word $w \in L$ representing $u \in M$ requires inserting only words from $G' \subset G$.

Now suppose that an insertion of depth greater than n^2 is required to obtain w from u . Then w factorizes as $w'apaqdrdw''$, where the first distinguished letter a and second distinguished letter d are the first and last letters of some inserted word of depth k , and the second distinguished letter a and first distinguished letter d are from some inserted word of depth $\ell > k$, and where the automaton \mathcal{A} enters the same state after reading the two distinguished letters a and enters the same state after reading the two distinguished letters d . (Such a factorization must exist because there are only n^2 possible pairs of states, and there are inserted words of depth exceeding n^2 .) Notice that $aqd \Rightarrow_{\mathcal{R}}^* \varepsilon$ and so $apaqdrd \Rightarrow_{\mathcal{R}}^* aprd \Rightarrow_{\mathcal{R}}^* \varepsilon$. Then, by the pumping lemma,

$$w'apapaqdrdrdw'' \in L,$$

but

$$w'apapaqdrdrdw'' \Rightarrow_{\mathcal{R}}^* w'apaprdrdw'' \Rightarrow_{\mathcal{R}}^* w'aprdw'' \Rightarrow_{\mathcal{R}}^* w'w'' \Rightarrow_{\mathcal{R}}^* u,$$

and so there are two representatives w and $w'apapaqdrdrdw''$ in L of $u \in M$. This is a contradiction and so shows the falsity of the assumption that insertions of depth greater than n^2 are required to obtain the representative in L of a normal form word in M .

Suppose that, in the process of performing insertions to obtain a representative $w \in L$ for an element $u \in M$, a word $w^{(k)}$ is obtained after the insertions of depth k have been performed. Suppose further that in performing the insertions of depth $k+1$, more than n insertions are made between consecutive letters of $w^{(k)}$ to obtain a word $w^{(k+1)}$. (The reasoning below also applies if $w^{(k)}$ is the empty word, which would require $k=0$.) Then $w^{(k+1)}$ factors as

$$w^{(k+1)} = v'ab^{\alpha_1}c^{\alpha_1}dab^{\alpha_2}c^{\alpha_2}d \dots ab^{\alpha_h}c^{\alpha_h}dv'',$$

where $h > n$, and each $ab^{\alpha_i}c^{\alpha_i}d$ is a word from G' . Then w factors as

$$w = w'ap_1dap_2d \dots ap_hdw'',$$

where $w' \Rightarrow_{\mathcal{R}}^* v'$, $w'' \Rightarrow_{\mathcal{R}}^* v''$, and $p_i \Rightarrow_{\mathcal{R}}^* b^{\alpha_i}c^{\alpha_i}$ for each i . Then \mathfrak{A} enters the same state on reading $w'ap_1dap_2d \dots ap_id$ and $w'ap_1dap_2d \dots ap_jd$ for some $i < j$. So by the pumping lemma,

$$q = w'ap_1dap_2d \dots ap_id(ap_{i+1}d \dots ap_jd)^2ap_{j+1}d \dots ap_kdw'' \in L.$$

But

$$\begin{aligned} q &= w'ap_1dap_2d \dots ap_id(ap_{i+1}d \dots ap_jd)^2ap_{j+1}d \dots ap_kdw'' \\ &\Rightarrow_{\mathcal{R}}^* v'ab^{\alpha_1}c^{\alpha_1}dab^{\alpha_2}c^{\alpha_2}d \dots \\ &\quad \dots ab^{\alpha_i}c^{\alpha_i}d(ab^{\alpha_{i+1}}c^{\alpha_{i+1}}d \dots \\ &\quad \dots ab^{\alpha_j}c^{\alpha_j}d)^2ab^{\alpha_{j+1}}c^{\alpha_{j+1}}d \dots ab^{\alpha_h}c^{\alpha_h}dv'', \\ &\Rightarrow_{\mathcal{R}}^* v'v'' \\ &\Rightarrow_{\mathcal{R}}^* u, \end{aligned}$$

and so there are two representatives w and q of the element $u \in M$. This contradicts the uniqueness of representatives in L and shows the falsity of the supposition that more than n insertions between consecutive letters in the process of obtaining a representative in L for an element of M .

Therefore, to sum up: a representative w in L of an element u of M can be obtained by inserting elements of G' to a depth of at most n^2 , with at most n consecutive words being inserted between adjacent letters at any stage. Notice that the maximum length of words in G' is $2n+2$. Thus, starting with empty word, the after depth 1 insertions, there are at most $n(2n+2)$ letters; after depth 2 insertions, at most $n^2(2n+2)^2$; and after depth n^2 insertions, at most $h = n^{n^2}(2n+2)^{n^2}$. Similarly, if one starts with a word u and performs insertions to obtain its representative in L , at most h new symbols are inserted between any adjacent pair of letters in u .

Define

$$H = \{w \in A^* : |w| \leq h, w \Rightarrow_{\mathcal{R}}^* \varepsilon\}.$$

Then, by the observations in the last paragraph, if $u \in M$ with $u = u_1 \dots u_n$ is represented by $w \in L$, then $w \in Hu_1Hu_2 \dots Hu_nH$. Define the rational relation

$$\mathcal{P} = (\{(a, a) : a \in A\} \cup \{(p, \varepsilon) : p \in H\})^*.$$

Then, since removing all subwords in H from a word in L yields the word to which it rewrites, it follows that

$$M = (L \circ \mathcal{P}) \cap (A^* - A^*HA^*) = \{u \in A^* - A^*HA^* : (\exists w \in L)((w, u) \in \mathcal{P})\},$$

and so M , which is the language of normal forms of (A, \mathcal{R}) , is regular.

However, two words $ab^\alpha c^\beta d$ and $ab^{\alpha'} c^{\beta'} d$ (where $\alpha, \beta, \alpha', \beta' \in \mathbb{N}$) represent the same element of M if and only if $\alpha = \beta$ and $\alpha' = \beta'$, in which case they both represent the identity of M . Thus, since in M the unique representative of the identity is ε , the language $K = ab^*c^*d - M$, which is also regular, consists of precisely those words of the form $ab^\alpha c^\beta d$ that represent the identity. That is, the language K is $\{ab^\alpha c^\alpha d : \alpha \in \mathbb{N}\}$, which is not regular by the pumping lemma. This is a contradiction, and so M does not admit a regular language of unique representatives. \square

5 REFERENCES

- [BO93] R. V. Book & F. Otto. *String-Rewriting Systems*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993.
- [Cai] A. J. Cain. ‘Hyperbolicity of monoids presented by confluent monadic rewriting systems’. Submitted. URL: www-groups.mcs.st-andrews.ac.uk/~alanc/publications/c_rshcg/c_rshcg.pdf.
- [CRRT01] C. M. Campbell, E. F. Robertson, N. Ruškuc, & R. M. Thomas. ‘Automatic semigroups’. *Theoret. Comput. Sci.*, 250, no. 1–2 (2001), pp. 365–391. DOI: [10.1016/S0304-3975\(99\)00151-6](https://doi.org/10.1016/S0304-3975(99)00151-6).
- [CS09] J. Cassaigne & P. V. Silva. ‘Infinite words and confluent rewriting systems: endomorphism extensions’. *Internat. J. Algebra Comput.*, 19, no. 4 (2009), pp. 443–490. DOI: [10.1142/S0218196709005111](https://doi.org/10.1142/S0218196709005111).
- [DG04] A. Duncan & R. H. Gilman. ‘Word hyperbolic semigroups’. *Math. Proc. Cambridge Philos. Soc.*, 136, no. 3 (2004), pp. 513–524. DOI: [10.1017/S0305004103007497](https://doi.org/10.1017/S0305004103007497).
- [ECH⁺92] D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson, & W. P. Thurston. *Word Processing in Groups*. Jones & Bartlett, Boston, Mass., 1992.
- [FK04] J. Fountain & M. Kambites. ‘Hyperbolic groups and completely simple semigroups’. In *Semigroups and languages*, pp. 106–132. World Sci. Publ., River Edge, NJ, 2004. DOI: [10.1142/9789812702616_0007](https://doi.org/10.1142/9789812702616_0007).
- [Gil02] R. H. Gilman. ‘On the definition of word hyperbolic groups’. *Math. Z.*, 242, no. 3 (2002), pp. 529–541. DOI: [10.1007/s002090100356](https://doi.org/10.1007/s002090100356).
- [Gro87] M. Gromov. ‘Hyperbolic groups’. In S. M. Gersten, ed., *Essays in group theory*, vol. 8 of *Math. Sci. Res. Inst. Publ.*, pp. 75–263. Springer, New York, 1987.
- [HKOT02] M. Hoffmann, D. Kuske, F. Otto, & R. M. Thomas. ‘Some relatives of automatic and hyperbolic groups’. In G. M. S. Gomes, J. É. Pin, & P. V. Silva, eds, *Semigroups, Algorithms, Automata and Languages (Coimbra, 2001)*, pp. 379–406. World Scientific Publishing, River Edge, N.J., 2002.
- [HU79] J. E. Hopcroft & J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley Publishing Co., Reading, Mass., 1979.